Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1410 03/09/12

~ Hacker Is Informant! ~ People Are Talking! ~ SOPA Vote Is Delayed!
~ 'Sabu' Is Double Agent ~ Hackers Publish Source ~ Yahoo: Deep Layoffs?
~ Pakistan To Censor Web? ~ Apple Unveils 4G iPad! ~ No to Social Search?

~ New iPad To Break Bank? ~ ~ If .com, Seizable!

-* Anonymous Downs Vatican Site *-
-* Feb Video Game Retail Sales Drop 20% *-
-* ISPs To Disrupt Access of Copyright Abusers *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

I apologize for a quick edition of A-ONE this week, as well as no commentary od any kind. Due to a death in the family, my thoughts are elsewhere and I am trying to deal with family matters

Until next time...

=~=~=~=

->In This Week's Gaming Section - February Video Game Retail Sales Drop 20%!
"""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

February Video Game Retail Sales Drop 20 Percent

U.S. retail sales of video games tumbled 20 percent in February as people cut spending on video games and systems in a month without big new game launches.

Sales fell to $1.06 billion last month from $1.33 billion in February 2011, according to market researcher NPD Group.

Sales of the games themselves dropped 23 percent to $464.4 million,

But NPD analyst Anita Frazier estimates that people spent an additional $550 million to $600 million on acquiring video content outside of brick-and-mortar retail stores. This includes spending on mobile games,

video game downloads and buying virtual items.

Hardware sales fell 18 percent to $381.4 million. Hardware includes game consoles such as the Wii and the Xbox 360 and handheld systems such as the Nintendo 3DS. NPD no longer discloses how many gaming systems get sold each month.

Sales of video game accessories such as game controllers declined 16 percent to $215.2 million. Accessories range from game controllers to the Xbox Live point card, which lets users pay for movies, games or extra game content through their Xbox 360 consoles.

The month's top-selling game was "Call of Duty: Modern Warfare 3" from Activision Blizzard Inc. Square Enix Inc.'s "Final Fantasy XIII-2" came in at No. 2.

Microsoft Corp.'s Xbox 360 was the best-selling console for the seventh month in a row. Microsoft said it sold 426,000 units in February.

Sony Corp.'s handheld PlayStation Vita launched in the U.S. on Feb. 22, and NPD said there were four days of retail sales for the gadget in the February sales report. With the Vita, video game console units rose 87 percent from January. Without it, hardware unit sales rose 62 percent.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Stop Online Piracy Act Vote Delayed

The House Judiciary Committee considering whether to send the Stop Online Piracy Act to the House floor abruptly adjourned Friday with no new vote date set - a surprise given that the bill looked certain to pass out of committee.

The committee s chairman and chief sponsor of the legislation, Rep. Lamar Smith (R-Texas), agreed to further explore a controversial provision that lets the Attorney General order changes to core internet infrastructure in order to stop copyright infringement.

Smith said the hearing would resume at the "earliest practical day that Congress is in session." Hours later, Rep. Darrell Issa (R-California) tweeted that the committee would resume action Wednesday.

The abrupt halt to Friday s proceeding, which followed a marathon-long, 11-hour hearing Thursday, was based on a motion from Rep. Jason Chaffetz (R-Utah). He urged Smith to postpone the session until technical experts could be brought in to testify whether altering the internet s domain-naming system to fight websites deemed 'dedicated' to infringing activity would create security risks.

Just yesterday, Smith said that was not necessary, despite a signed letter by many of the internet s core engineers saying the bill s approach was technically flawed.

The legislation mandates that ISPs alter records in the net s system for looking up website names, known as DNS, so that users couldn t navigate to the site. Or, if ISPs choose not to introduce false information into DNS at the urging of the Justice Department, they instead would be required to employ some other method, such as deep-packet inspection, to prevent American citizens from visiting infringing sites.

ISPs, could, for instance, adopt tactics used by the Great Chinese Firewall to sniff for traffic going to a blacklisted site and simply block it.

But a host of security researchers and tech policy experts, including Stewart Baker, the former Department of Homeland Security policy director, said the plan "would still do great damage to internet security."

On Thursday, Chaffetz and a host of other lawmakers asked Smith to stop the hearing so that the committee could bring in experts to testify. But Smith had refused, and the committee voted 22-12 to leave the DNS redirect and firewall provisions intact.

The committee heard from the Motion Picture Industry Association of America at a SOPA hearing last month, but has never called an expert on internet architecture. It was not immediately clear who Smith would ultimately line up.

Michael O Leary, an MPAA vice president, had testified last month before the committee that security concerns were ’overstated.’

Putting false information into the DNS system - the equivalent of the net s phonebook - would be ineffective, frustrate security initiatives and lead to software workarounds, according to a paper co-signed by security experts Steve Crocker of Shinkuro, David Dagon of Georgia Tech, Dan Kaminsky of DKH, Danny McPherson of Verisign and Paul Vixie of Internet Systems Consortium. The paper was lodged into the committee s record on Thursday.

"These actions would threaten the Domain Name System s ability to provide universal naming, a primary source of the internet s value as a single, unified, global communications network," they wrote.

Also lodged into the record was an open letter from 83 prominent internet engineers, including Vint Cert, John Gilmore and L. Jean Camp.

"The US government has regularly claimed that it supports a free and open internet, both domestically and abroad. We cannot have a free and open Internet unless its naming and routing systems sit above the political concerns and objectives of any one government or industry," they wrote.

In the security context, they maintain the bill would break the internet s universal character and hamper U.S. government-supported efforts to rollout out DNS-SEC, which is intended to prevent hackers from hijacking the net through fake DNS entries.

The measure, meanwhile, also grants private companies the ability to de-fund websites they allege to be trafficking in unauthorized copyright and trademark goods. Rights holders may ask judges to order ad networks and banks to stop doing business with a site dedicated to infringing

activities.

The legislation also gives legal immunity to financial institutions and ad networks that choose to boycott the rogue sites even without having been ordered to do so.

Smith s legislation targets sites with foreign domains, not American-based ones ending in .com, .org and .net.

Hackers Busted After 1 Becomes FBI Informant

An Internet outlaw’s decision to go to work for the FBI poured light on a secretive world where young computer experts caused havoc and where authorities say a Chicago man and others celebrated their successes as they stole hundreds of thousands of dollars with stolen credit card numbers.

Court documents unsealed Tuesday revealed charges against six individuals in Europe and the United States and showed the clash between law enforcement and Internet hackers, a group of worldwide computer enthusiasts already threatening to retaliate.

Law enforcement officials said it marked the first time core members of the loosely organized worldwide hacking group Anonymous have been identified and charged in the U.S.

Some Anonymous members put on a brave face.

"Anonymous is a hydra, cut off one head and we grow two back," read one defiant message posted to Twitter.

At the center was the legendary hacker known as "Sabu," who when he was arrested last June was identified as Hector Xavier Monsegur, 28, a self-taught, unemployed computer programmer with no college education. Authorities said his cooperation has helped to prevent more than 300 Internet attacks.

Authorities said he was living on welfare in public housing in New York as he carried out crimes that made him a hero to some in cyberspace until he made a rookie mistake - he posted something online without cloaking his IP address, or computer identity - and someone tipped off the FBI.

Court records show he agreed to cooperate during an August plea proceeding and testify against others.

Among those charged Tuesday was 27-year-old Jeremy Hammond of Chicago. Investigators said Hammond boasted that he’d snared the personal data of a former U.S. vice president and one-time CIA director as part of an attack in December of Strategic Forecasting Inc. or Stratfor, a global intelligence firm in Austin, Texas, that affected up to 860,000 victims.

The government said Hammond conspired to hack into computer systems used by Stratfor, which describes itself as a subscription-based provider of geopolitical analysis.

It said he and co-conspirators stole credit card information for approximately 60,000 credit card users and used some of the stolen data to

make more than $700,000 in unauthorized charges.

Court papers said a January email titled "Official Emergency Communique Straight from the Anonymous Hacker Underground" was sent to the company's customers whose accounts had been compromised. The papers said it claimed: "The sheer amount of destruction we wreaked on Stratfor's servers is the digital equivalent of a nuclear bomb: leveling their systems in such a way that they will never be able to recover."

Investigators said Monsegur and the other defendants were associated with Anonymous, and some were also part of the elite spinoff organization that Monsegur formed last May, Lulz Security or LulzSec. "Lulz" is Internet slang for "laughs" or "amusement."

Monsegur and the other defendants were accused in court papers of hacking into corporations and government agencies around the world, including the U.S. Senate, filching confidential information, defacing websites and temporarily putting victims out of business. Authorities said more than 1 million people were affected.

Prosecutors said that among other things, the hackers, with Monsegur as their ringleader, disrupted websites belonging to Visa, Mastercard and Paypal in 2010 and 2011 because the companies refused to accept donations to Wikileaks, the organization that spilled a trove of U.S. military and diplomatic secrets.

Also, prosecutors said, Monsegur and the others attacked a PBS website last May and planted a false story that slain rapper Tupac Shakur was alive in New Zealand. Investigators said it was retaliation for what the hackers perceived to be unfavorable news coverage of Wikileaks on the PBS program "Frontline."

A Twitter account associated with Monsegur has some 45,000 followers and regularly spouts expletive-filled anti-government messages. His last tweet on Monday was in German. An earlier tweet described the federal government as being run by "cowards."

"Don't give in to these people," the message read. "Fight back. Stay strong."

Monsegur pleaded guilty in August to charges that included conspiracy to commit hacking, admitting he obtained dozens of credit card numbers online and gave them to others or used them to pay his bills. His lawyer, Philip L. Weinstein, declined to comment Tuesday.

His deal with prosecutors requires his full cooperation and testimony at any trial. In return, he gets leniency from a potential prison sentence of more than 120 years. He is free on $50,000 bail.

Also charged with conspiracy to commit computer hacking were Ryan Ackroyd, 25, of Doncaster, England; Jake Davis, 19, of Lerwick, Scotland; Darren Martyn, 25, of Galway, Ireland, and Donncha O'Cearrbhail, 19, of Birr, Ireland.

Davis' lawyer, Adel Buckingham, declined comment. Contact information for the other European defendants' lawyers could not immediately be located.

Hammond, who was arrested Monday, appeared before a federal judge in Chicago and was ordered transferred to New York.

Defense attorney Jim Fennerty described Hammond as compassionate, saying he had rallied against plans to hold the 2016 Olympics in Chicago because he felt it would hurt low-income people and had protested against neo-Nazi groups.

"He’s concerned about people and issues - that’s why I like him," Fennerty said.

In July, when LulzSec’s attacks were grabbing world headlines, someone alleged that Sabu was Monsegur and posted personal details about him on the Internet. Sabu took to Twitter to deny it.

Barrett Brown, a former journalist who became closely associated with Anonymous, said Sabu’s cooperation with the FBI could do serious damage to Anonymous.

"He was an admired Anon," he said. "He’s been a leader. People came to him with information. God knows what else he told them."

Hacker Arrested in NYC Cooperated from Day 1

In his Twitter postings, the elite computer hacker known as "Sabu" urged followers to resist the U.S. government and its agents.

But court papers made public Thursday reveal that Hector Xavier Monsegur put up no such fight when FBI agents first knocked on his door on June 7. From almost that first moment, he began talking, naming names and helping investigators pick apart the international community of Internet saboteurs.

He was arrested at 10:15 p.m. By the next day, federal prosecutors had told a judge that Monsegur had given them detailed information on other hackers suspected of breaking into the computer systems at several big corporations.

"Since literally the day he was arrested, the defendant has been cooperating with the government proactively," Assistant U.S. Attorney James Pastore told a judge in New York during a secret court session for Monsegur on Aug. 5. Over the past few months, the prosecutor said: "The defendant has literally worked around the clock with federal agents. He has been staying up sometimes all night engaging in conversations with co-conspirators that are helping the government to build cases against those co-conspirators."

That cooperation resulted in the arrests of five other alleged hackers this week in Ireland, Scotland, England and the U.S., a takedown that stunned fellow Internet saboteurs known for prizing anonymity and a culture of resistance.

Monsegur secretly pleaded guilty in August, but judges had agreed to close public courtrooms and seal all records of his case in order to keep his work with the government from becoming known. Most of those court files have since been unsealed, and documents made available Thursday provided a handful of new details about Monsegur’s work.

While software on his computer tracked his online activity and video cameras monitored his home at a New York City public housing project,

prosecutors said, Monsegur worked feverishly with the FBI to monitor Internet communications between fellow hackers. In many cases, he helped thwart attacks as they were being planned, prosecutors said in a court filing.

By August, he had worked with the FBI to "patch" 150 vulnerabilities in computer systems being eyed by hackers, or in other cases react quickly to help attack victims mitigate the damage, Pastore said in court.

Prosecutors were concerned from the start with Monsegur's safety if his identity were to be revealed.

"Some of the groups against whom the defendant is cooperating are known to retaliate against people who cooperate with the government in ways ranging from the mundane, for example, ordering hundreds of pizzas to someone's house, to much more serious: calling in hostage situations in part by using family information and having a SWAT team show up at the person's home," Pastore told a judge on Aug. 5.

Prosecutors haven't explained publicly why Monsegur was so willing to work with the government, even as he continued to rail against it in posts online. But court records did note that the 28-year-old was the legal guardian of two young nieces. Neighbors have told The Associated Press that Monsegur was raising the children after his aunt was jailed on drug charges.

Other court papers noted that Monsegur lived on meager means. He had been earning $6,000 per month until losing his job in the spring of 2010, and had since been living off of $400 unemployment checks.

Monsegur has yet to be sentenced for his computer crimes, which included a number of attacks on big corporations, foreign governments and U.S. government agencies.

Hackers Group Anonymous Take Down Vatican Website

The Italian branch of the hackers group Anonymous took down the Vatican's website on Wednesday, saying it was an attack on the Roman Catholic Church's scandals and conservative doctrine.

The Vatican website www.vatican.va was inaccessible. A spokesman said he could not confirm that the crash was the work of the hackers group but said technicians were working to bring it back up.

A statement on the Italian website of the loosely-knit cyber-activists group accused the Church of being responsible for a long list of misdeeds throughout history, including the selling of indulgences in the 16th century and burning heretics during the Inquisition.

"Today, Anonymous has decided to put your site under siege in response to your doctrine, liturgy and the absurd and anachronistic rules that your profit-making organization spreads around the world," the website said.

It also accused the Vatican of being "retrograde" in its interfering in Italian domestic affairs "daily."

Anonymous, along with another group LulzSec, has taken credit for a number

of high-profile hacking actions against companies and institutions, including the CIA.

Symantec Says Hackers Released Norton Source Code

Hackers have published the blueprints to a 2006 version of Symantec Corp's widely used Norton Antivirus software on the Internet, according to the software maker.

Symantec spokesman Cris Paden said on Friday that the release of the source code, during the last 24 hours, posed no risk to millions of Norton customers around the world whose PCs are protected by its security software.

"The code that has been exposed is so old that current out-of-the-box security settings will suffice against any possible threats that might materialize as a result of this incident," he said.

Symantec has previously disclosed that a group called Lords of Dharmaraja that is affiliated with the hacker group Anonymous was in possession of source code for several of its products. It said the code was obtained in a 2006 breach of the company's networks.

The hackers have previously released the source code for two other Symantec products: Norton Utilities and pcAnywhere.

The company initially urged customers to disable pcAnywhere in the wake of release of that product's source code, then it issued an upgrade to the software and said told customers it was safe to use again.

ISPs To Disrupt Internet Access of Copyright Scofflaws

The nation s major internet service providers, at the urging of Hollywood and the major record labels, have agreed to disrupt internet access for online copyright scofflaws.

The deal, almost three years in the making, was announced early Thursday, and includes participation by AT&T, Cablevision Systems, Comcast, Time Warner and Verizon. After four copyright offenses, the historic plan calls for these companies to initiate so-called 'mitigation measures' (.pdf) that might include reducing internet speeds and redirecting a subscriber s service to an 'educational' landing page about infringement.

The internet companies may eliminate service altogether for repeat file sharing offenders, although the plan does not directly call for such drastic action.

The agreement, backed by the Recording Industry Association of America and the Motion Picture Association of America, also does not require internet service providers to filter copyrighted material sailing through peer-to-peer protocols. U.S. internet service providers and the content industry have openly embraced filtering, and the Federal Communications Commission has all but invited the ISPs to practice it.

"This is a sensible approach to the problem of online content theft," said Randal Milch, Verizon s general counsel. Cary Sherman, the RIAA s president, said the deal was ’groundbreaking’ and "ushers in a new day and a fresh approach to addressing the digital theft of copyrighted works."

The RIAA, which includes Universal Music Group Recordings, Warner Music Group, Sony Music Entertainment and EMI Music North America, kicked off the marathon negotiations in December 2008, when it abruptly stopped a litigation campaign that included around 30,000 lawsuits targeting individual file sharers.

Key leverage in the marathon negotiations included the Digital Millennium Copyright Act, which demands that ISPs have a termination policy in place for repeat infringers. New York Governor Andrew Cuomo brought the parties together when he was that state s attorney general.

Michael O Leary, an MPAA vice president, said the industry will continue to push for federal legislation that would dramatically increase the government s legal power to disrupt and shutter websites dedicated to infringing activities. That legislation is blocked in the Senate.

"That is an important priority," he said during a telephone conference, noting that a House version of the stalled Senate legislation is to be introduced soon. The White House applauded Thursday s announcement, saying it will "have a significant impact on reducing online piracy."

The Center for Democracy & Technology, along with Public Knowledge, said in a joint statement they were concerned about the accord. "We believe it would be wrong for any ISP to cut off subscribers, even temporarily, based on allegations that have not been tested in court," the groups said.

Corynne McSherry, the intellectual property director at the Electronic Frontier Foundation, also had concerns. She added, in a telephone interview, that the EFF was "pretty disappointed that ISPs have agreed to serve as a propaganda agent for big media."

Thursday s plan, meanwhile, provides no immunity for internet subscribers facing legal action, and leaves it up to the rights holders to detect infringement.

"As provided under current law, copyright owners may also seek remedies directly against the owner of an internet account based on evidence they may collect," according to the deal. Sherman said in the telephone conference that the RIAA does "not rule out the possibility of bringing litigation" against repeat file sharing offenders.

The Copyright Act allows damages of up to $150,000 per infringement. Peer-to-peer file sharing of copyrighted works is easily detectable, as IP addresses of internet customers usually reveal themselves during the transfer of files.

On the first offense, internet subscribers will receive an e-mail ’alert’ from their ISP saying the account ’may have been’ misused for online content theft. On the second offense, the alert might contain an ’educational message’ about the legalities of online file sharing.

On the third and fourth infractions, the subscriber will likely receive a pop-up notice "asking the subscriber to acknowledge receipt of the alert."

After four alerts, according to the program, ’mitigation measures’ may commence. They include "temporary reductions of internet speeds, redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright, or other measures (as specified in published policies) that the ISP may deem necessary to help resolve the matter."

Online infringement, according to the MPAA and RIAA, accounts for thousands of lost jobs and billions of dollars in lost wages and taxes annually.

Members of the MPAA include Walt Disney Studios, Paramount Pictures, Sony Pictures, Twentieth Century Fox, Universal City Studios and Warner Bros.

Apple Unveils 4G iPad

Apple Inc’s latest iPad sports a crisper display and an array of technology advances that, while less than revolutionary, may prove enough for now to keep rivals like Amazon.com Inc and Samsung Electronics Co Ltd at bay.

While stopping short of vaulting ahead of Motorola and Samsung, the device - which comes 4G-ready and boasts a quad-core graphics processor - is capable enough to help safeguard its two-thirds market share. "The screen is a notable feature for non-techie customers, as is the faster connectivity. That’s something that mainstream consumers can identify with," said Morningstar analyst Michael Holt. "There’s pent-up demand because a new device was widely anticipated. I they’ve made enough incremental improvements to do well."

Other analysts say the faster processing may begin to draw heavy gamers, encroaching on turf now dominated by gaming-hardware makers such as Microsoft or Sony.

Chief Executive Tim Cook, presiding over his second major product launch after debuting with 2011’s voice-enabled iPhone 4S, introduced the highly anticipated third iteration of the tablet, which is available for pre-orders from Wednesday and will hit store shelves March 16.

But he stumped many in the audience by breaking away from the tradition of calling the third-generation tablet the iPad 3, as some had expected, referring to it simply as the "new iPad."

The company said it will continue to sell the iPad 2 but dropped its price by $100. The older tablet now starts at $399 while the new third-generation wi-fi only iPad starts at $499.

The high-end model of Apple’s latest iPad starts at $629 and will be capable of operating on a high-speed 4G "LTE," or Long-Term Evolution, network. At speeds roughly 10 times faster than current 3G technology, that may help banish the sometimes shaky video quality of older devices.

Wall Street had anticipated many of the features Cook showed off on Wednesday, including a higher-definition "retina display" screen - containing several times as many pixels within the same area - and a better camera.

Shares of Apple closed barely higher, up 43 cents at $530.69. They hovered around $530 throughout the unveiling event, which was attended by Marc Benioff, CEO of enterprise cloud computing company Salesforce.com Inc; Jeremy Stoppelman, CEO of online business review site Yelp Inc; and influential venture-capitalist John Doerr, among other industry luminaries.

Some had held out hope of a positive Apple surprise, recalling late CEO Steve Jobs and his now-iconic "one more thing" at the very end of such announcements. Others said the upgrades and tweaks to the iPad could only go so far in fending off hard-charging competition.

"While the hardware is notably enhanced, with an impressive retina display, better camera and faster processor, there are still some areas of improvement that Apple needs to work on, in order to stay ahead of its encroaching competitors," said Fred Huet, managing partner at Greenwich Consulting.

"As tablets are increasingly being used for personal media consumption, it is promising to see a better screen resolution. But will this be enough to ensure Apple’s competitive lead in the marketplace? No."

Others say Apple is betting a 4G-equipped iPad will tempt more U.S. consumers to pay for higher-quality video on the go. That, in turn, should give Verizon Wireless and AT&T Inc a revenue boost, analysts say.

Verizon Wireless, a venture of Verizon Communications Inc. and Vodafone Group Plc, and AT&T will host and sell 4G wireless plans to 4G iPad users.

Until now, buyers have been reluctant to shell out extra cash even for iPads with slower 3G connections. The cheaper WiFi-only model, with much more limited Web access, is by far Apple’s top-selling one today.

An updated version of the WiFi-only model remains at $499. The most expensive 4G model, with 64 gigabytes of storage, will go for $829. The previous iPad2 with 3G also sold for $629 to $829. The cheapest model of the previous-generation iPad 2 now retails at $399.

"The iPhone 4S showed us that Apple doesn’t need to out-do itself with new product designs to continue extending its domination of a category," said CCS Insight analyst John Jackson.

In an apparent departure from naming conventions, Apple’s third-generation tablet will not be called the iPad 3, but simply referred to as the latest iPad, a small point that several analysts and executives noticed and pointed out.

Forrester analyst Frank Gillet said most of Apple’s other products, such as the iPod or the MacBook Pro, do not warrant new appellations every time they go through an upgrade. Apple may even drop the numerical extension for the iPhone, he added.

Regardless of the name, the company is counting on a warm reception to its latest tablet to fend off an increasingly aggressive challenge from tablets powered by Google Inc’s Android technology, with Microsoft Corp software-driven devices slated to come soon. "Everyone’s been wondering who will come out with a product that’s more amazing than the iPad 2," Cook said.

"Stop wondering: We are."

Earlier in the proceedings, Cook again held forth on what he called a "post-PC world," in which users move increasingly away from traditional desktop and laptop computing and toward an array of portable devices, including tablets.

Smartphones and tablets are starting to eat into PC sales as mobile technology gets more advanced and available content expands.

Some experts believe mobile devices, as they get more powerful, will eventually displace PCs in many markets, hurting business for the likes of Hewlett-Packard Co and Dell Inc.

The global tablet user base reached 67 million in 2011, according to researcher Strategy Analytics. Analysts expect double-digit growth in tablet sales in coming years.

Cook also announced that the company’s new $99 Apple TV set-top box, a concept that late CEO Steve Jobs had called a "hobby," now supports high-definition 1080p screen technology.

"Last year alone we sold 172 million post-PC devices," Cook told the audience at the Yerba Buena Center in downtown San Francisco, Apple’s preferred venue for product unveilings.

"And this made up 76 percent of our revenues. This is incredible."

Cook’s performance was again the subject of scrutiny. The CEO replaced famed showman Jobs after the co-founder’s October death, and has since drawn several comparisons in terms of onstage charisma.

Some in Wednesday’s audience found the event wanting.

"This iPad 3 launch is horribly boring. Steve, I miss you terribly," Salesforce’s Benioff tweeted at the end of the proceedings. "Tim Cook didn’t thank or remember Steve Jobs at iPad3 launch. There would be no iPad 3 without Steve Jobs."

Apple s New iPad Can Max Out Your Data Plan in 10 Minutes

The new iPad is here, but will its speed cost you big?

One of the hallmark features of Apple’s new iPad is its support for faster 4G mobile networks from carriers Verizon and AT&T, and from experience you will certainly benefit from truly impressive data speeds as a result. Unfortunately, all that blazing speed is going to come at a blazingly high price to match.

As the graphic below shows, you’ll be paying the same price for either 2GB or 5GB worth of monthly data on either carrier at $30 and $50 monthly, respectively; AT&T also offers a smaller 250MB plan for $14.99, and Verizon offers a higher 10GB plan for $80 per month. The trouble is, none of those data caps are actually very high when you start factoring things in like streaming video, audio, beaming high-resolution photographs (one of the features in the new iPhoto for iPad application), or syncing all of your various media files using Apple’s own iCloud storage service. Even some apps, particularly games, can clock in at hundreds of megabytes.

Combine the realities of multimedia file size and a blazing fast connection that allows transfer of said files at unprecedented speeds, and you have a recipe for potentially expensive disaster. One careless download of a 1080p high-definition movie from the iTunes Store over 4G could eat up your entirely monthly plan and then some. In fact, if you could achieve download speeds at the theoretical maximum 72Mbps of LTE, you could blow through a 5GB plan in just under 10 minutes, and Verizon's largest 10GB tier in about 20. Real-world speeds of course are actually going to be somewhat lower, but we're still talking about the potential to obliterate your entire expensive monthly data plan in much less than a single day.

Data pricing remains the Achilles' heel of 4G. Carriers and manufacturers alike are avidly attempting to seduce consumers with the allure of always-on connectivity offering speeds comparable to, if not faster than, our cable internet service at home - but both sticker and bandwidth shock are going to increasingly confront the average consumer as devices like the new iPad spur greater interest in and adoption of 4G service. To live up to the true promise of 4G, carriers will need to stop pricing mobile data for gentle sipping and find a way to offer reasonable plans that reflect real-world usage of 4G devices.

'Deep' Layoffs Expected at Yahoo

According to All Things Digital's Kara Swisher, "multiple sources both inside and outside" Yahoo say that Thompson "is preparing a massive restructuring of the company, including layoffs that are likely to number in the thousands."

Yahoo is no stranger to layoffs in recent years. It cut about 150 jobs in January 2011, after hacking 650 to 700 full-time positions a month earlier. And in 2008, about 1,600 Yahoo employees lost their jobs.

That was the year Yahoo's board realized it couldn't turn around the company with co-founder Jerry Yang at the helm. So the board hired former Autodesk CEO Carol Bartz in January 2009. Within four months, she had cut 5% of Yahoo's workforce, or 675 jobs, as part of her well-articulated strategy to enable the company to "kick some butt." She should have specified whose butts were in for a kicking.

Now it sounds like Thompson, who became CEO in early January, four months after Bartz's own butt got kicked, is planning to hack even deeper.

Yahoo currently has about 14,100 employees, almost exactly how many it had in November 2010, despite subsequent layoffs. From Swisher's report, it sounds like every division and project at Yahoo must make an economic case for its survival, both product and non-product (PR, marketing, research).

Supposedly layoffs and organizational restructuring could be announced by the end of March. Don't be surprised if there are more in the months after; it seems as if Thompson is willing to make big changes.

Yahoo, of course, has had stagnant revenue and share price for several years now as it has been eclipsed by Google and Facebook as a favorite destination for online advertisers. This has led to shareholder uprisings and turmoil on the board, from which four directors last month

announced their resignation.

Last September I wrote a post titled, "Now would be an excellent time for Yahoo employees to jump ship." I hope some of them did. To those who didn't, good luck.

Wanted: Censor for Pakistan's Internet

Pakistan is advertising for companies to install an Internet filtering system that could block up to 50 million Web addresses, alarming free speech activists who fear current censorship could become much more widespread.

Internet access for Pakistan's some 20 million Web users is less restricted than in many countries in Asia and the Arab world, though some pornographic sites and those seen as insulting to Islam are blocked. Others related to separatist activities or army criticism have also been, or continue to be, censored.

Few nations have so publicly revealed their plans to censor the Web as Pakistan is doing, however. Last month, the government took out newspaper and Web advertisements asking for companies or institutions to develop the national filtering and blocking system.

"They are already blocking a lot of Internet content, and now they are going for a massive system that can only limit and control political discourse," said Shahzad Ahmad, the director of Bytes for All Pakistan, which campaigns for Internet freedom. "The government has nothing to do with what I choose to look at."

The government doesn't currently list the sites it has blocked, or their number, or say who sits on the committee that decides what pages to shut down. Pakistan's Telecommunication Authority instructs the country's 50 Internet Service Providers to block sites. The ISPs, which receive their license from the PTA, are obliged to obey.

In November, the PTA ordered cell phone companies to block text messages containing a list of more than 1,500 English words it said were offensive. But the plan was dropped after public ridicule and complaints from cell phone companies about practicality.

The plan to censor the Internet comes amid unease over a set of proposals by a media regulatory body aimed at bringing the country's freewheeling television media under closer government control. With general elections later this year or earlier next, some critics have speculated the government might be trying to cut down on criticism.

The media proposals call for television stations not to broadcast programs "against the national interest" or those that "undermine its integrity or solidarity as an independent and sovereign country" or "contain aspersions against or ridicule the organs of the State."

Pakistan's Information Minister Firdous Ashiq Awan denied Wednesday that the government was seeking to curb the media.

"We want to see the media growing. We want to strengthen it," Awan said, emphasizing that the proposals were just that, and the government wouldn't

implement them without the media’s consent.

The government advertisements state it wants a system capable of shutting down up to 50 million Web addresses in multiple languages with a processing delay of not less than one millisecond.

The head of Pakistan’s ISP association, Wahajus Siraj, said he supported the proposed system, saying his ISP and others in the association didn’t have the time or money to take down the sites. He also said rights activists had nothing to worry about.

"They don’t fully understanding the concept of it," said Siraj. "This is not new censorship. It’s making the manual system more efficient. I respect their point of view, but decent freedom of speech should not be blocked."

Siraj, who sits on the board of the government-run technology fund seeking proposals for the blocking system, said there had been many expressions of interest to create the system, including from two Western firms. He declined to name them.

Websense Inc., a San Diego-based Internet security firm, has already said it is not bidding for the Pakistan project.

"We call on other technology providers to also do the right thing for the citizens of Pakistan and refuse to submit a proposal for this contract," it said in a statement. "Broad government censorship of citizen access to the Internet is morally wrong."

U.S. technology companies have been criticized for helping foreign governments censor the Internet to their citizens. Cisco Systems Inc., which makes networking equipment that could be used in official efforts to monitor and control Internet use, is often cited; the company insists it does not provide any government with any special capabilities and cannot control what its customers do with the products.

Like in many Asian countries where pornographic materials are banned, Pakistan currently tries to block adult websites. It also seeks to censor what it sees as "blasphemous" content toward Islam, as other Muslim nations do.

In 2008, the government blocked YouTube because of anti-Islamic movies on the site; in 2010, it blocked Facebook for two weeks amid anger over a page that encouraged users to post images of Islam’s Prophet Muhammad.

Other sites that have, or continue to be blocked, are those containing news and views from Baluchistan, a southwestern province where a separatist insurgency has simmered for years in the face of army crackdowns. There have been other cases where sites have been blocked apparently after they triggered the anger of members of the military and political elite. Rollingstone.com has been offline since July last year, reportedly because it ran a short story critical of the amount of budgetary funds allocated to the army. Rollingstone.com didn’t return e-mails seeking comment.

Asked for comment, the telecommunication authority sent a statement that explained the blocking system was being installed because the Pakistani people wanted a "ban on blasphemous and objectionable contents that were being used to harass, deface and blackmail the innocent citizens of Pakistan."

Blocking pornographic websites and those seen insulting to Islam is not unpopular in Pakistan; many would say it is obligatory under Islam. Many of the most high-profile blocks have been a result of court orders acting on petitions from members of the public.

"I’m with the government on this one. They have right the intention," said Ahmjad Alvi, founder of Brainnet, one of the country’s first ISPs. "Think of the kids."

Nobody Really Likes Social Search Besides Google

Though Google claims the search process has been made better with its new social search, people don’t want that type of personalized experience while searching, at least according to a new Pew study. Social search, in Google’s eye, enhances the experience; they assume we want to see what our friends have posted on their Google+ profiles. It might make planning a trip more informed, for example. But, actually it’s just clutter. The only one that benefits from the setup is Google.

The problem is, social search doesn’t really provide the right kind of information. We learned this when we tested the new Google out a few weeks ago, getting very few relevant results for our queries. 65 percent of those asked by Pew agreed, saying personalized search was a "bad thing" - not for the usual privacy concerns, but because "it may limit the information you get online and what search results you see." There were the privacy issues too, with 73 percent of those surveyed not OK with it on those grounds.

Even though Google claims to have a "better product," there’s an irrelevancy issue here; the company, in part, brought that upon itself when it decided to leave every other social network out of its game. Those Google+ profiles don’t provide the same wealth of information bigger-name social networks like Twitter or Facebook do, and Google social search only includes Google+. The other issue, however, is that when searching Google, people want the right answers to questions, from expert-ish sources - not pictures of their friends’ kids.

Google personalizes search in other, more subtle ways than just Google+, and has been doing so for more than two years, tracking sites we often click to provide "better" results. Social search brings personalization to a whole new level, though, increasing both the visibility and volume of targeted search results.

While users grumble, Google pushes forward because personalized results mean more direct advertising. Advertisers like that, and Google lives off of advertising.

Uncle Sam: If It Ends in .Com, It s .Seizable

When U.S. authorities shuttered sports-wagering site Bodog.com last week, it raised eyebrows across the net because the domain name was registered with a Canadian company, ostensibly putting it beyond the reach of the U.S. government. Working around that, the feds went directly to VeriSign, a U.S.-based internet backbone company that has the contract to manage

the coveted .com and other ’generic’ top-level domains.

EasyDNS, an internet infrastructure company, protested that the "ramifications of this are no less than chilling and every single organization branded or operating under .com, .net, .org, .biz etc. needs to ask themselves about their vulnerability to the whims of U.S. federal and state lawmakers."

But despite EasyDNS and others outrage, the U.S. government says it s gone that route hundreds of times. Furthermore, it says it has the right to seize any .com, .net and .org domain name because the companies that have the contracts to administer them are based on United States soil, according to Nicole Navas, an Immigration and Customs Enforcement spokeswoman.

The controversy highlights the unique control the U.S. continues to hold over key components of the global domain name system, and rips a Band-Aid off a historic sore point for other nations. A complicated web of bureaucracy and Commerce Department-dictated contracts signed in 1999 established that key domains would be contracted out to Network Solutions, which was acquired by VeriSign in 2000. That cemented control of all-important .com and .net domains with a U.S. company - VeriSign - putting every website using one of those addresses firmly within reach of American courts regardless of where the owners are located - possibly forever.

The government, Navas said, usually serves court-ordered seizures on VeriSign, which manages domains ending in .com, .net, .cc, .tv and .name, because "foreign-based registrars are not bound to comply with U.S. court orders." The government does the same with the non-profit counterpart to VeriSign that now manages the .org domain. That s the Public Interest Registry, which, like VeriSign, is based in Virginia.

Such seizures are becoming commonplace under the Obama administration. For example, the U.S. government program known as Operation in Our Sites acquires federal court orders to shutter sites it believes are hawking counterfeited goods, illegal sports streams and unauthorized movies and music. Navas said the U.S. government has seized 750 domain names, "most with foreign-based registrars."

VeriSign, for its part, said it is complying with U.S. law.

"VeriSign responds to lawful court orders subject to its technical capabilities," the company said in a statement. "When law enforcement presents us with such lawful orders impacting domain names within our registries, we respond within our technical capabilities."

VeriSign declined to entertain questions about how many times it has done this. It often complies with U.S. court orders by redirecting the DNS (Domain Name System) of a domain to a U.S. government IP address that informs online visitors that the site has been seized (for example, ninjavideo.net.)

"Beyond that, further questions should be directed to the appropriate U.S. federal government agency responsible for the domain name seizure," the company said.

The Public Interest Registry did not immediately respond for comment.

Bodog.com was targeted because federal law generally makes it illegal to

offer online sports wagering and to payoff online bets in the United States, even though online gambling isn t illegal globally.

Bodog.com was registered with a Canadian registrar, a VeriSign subcontractor, but the United States shuttered the site without any intervention from Canadian authorities or companies.

Instead, the feds went straight to VeriSign. It s a powerful company deeply enmeshed in the backbone operations of the internet, including managing the .com infrastructure and operating root name servers. VeriSign has a cozy relationship with the federal government, and has long had a contract from the U.S. government to help manage the internet s 'root file' that is key to having a unified internet name system.

Still, the issue of the U.S. s legal dominion claim over all .com domains wasn t an issue in the January seizure of the domain of megaupload.com, which is implicated in one of the largest criminal copyright cases in U.S. history. Megaupload.com was registered in the United States with a registrar based in Washington state.

The United States would have won even more control over the internet with the Stop Online Piracy Act and the Protect IP Act. But the nation s biggest online protest ever scuttled the measures, which would have allowed the government to force internet service providers in the U.S. to prevent Americans from being able to visit or find in search engines websites that the U.S. government suspected violated U.S. copyright or trademark law.

But as the Justice Department demonstrated forcefully with the takedown of Megaupload, just a day after the net s coordinated anti-SOPA protest, it still has powerful weapons to use, despite the deaths of SOPA and PIPA.

So how does International Corporation for Assigned Names and Numbers, the global body that oversees the domain-naming system, feel about the U.S. government s actions? ICANN declined comment and forwarded a 2010 blog post from it s chief Rod Beckstrom, who said ICANN has "no involvement in the takedown of any website."

ICANN, a non-profit established by the U.S., has never awarded a contract to manage the .com space to a company outside the United States - in fact VeriSign has always held it - despite having a contentious relationship with ICANN that s involved a protracted lawsuit. But, due to contract terms, VeriSign is unlikely to ever lose control over the immensely economically valuable .com handle.

ICANN is also seeking to distance itself from the U.S. government by being more inclusive, including allowing domain names in a range of written, global languages, ending the exclusivity of the Latin alphabet in top-level domains.

Still, many outside the United States, like China, India and Russia, distrust ICANN and want control of the net s naming system to be turned over to an organization such as the International Telecommunications Union, an affiliate of the United Nations. Last year, Russian Prime Minister Vladimir Putin met with Hamadoun Toure, the ITU s chief, and said he wanted international control over the internet "using the monitoring capabilities of the International Telecommunication Union."

"If we are going to talk about the democratization of international relations, I think a critical sphere is information exchange and global control over such exchange," Putin said, according to a transcript from

the Russian government.

Just last week, Robert McDowell, a Federal Communications Commission commissioner, blasted such an idea.

"If successful, these efforts would merely imprison the future in the regulatory dungeon of the past," he said. "Even more counterproductive would be the creation of a new international body to oversee internet governance."

ICANN was established in 1998 by the Clinton administration, and has been under global attack to internationalize the control of the Domain Name System ever since. A United Nations working group in 2005 concluded that "no single government should have a pre-eminent role in relation to international internet governance."

But those pressures don t seem to have registered with President Barack Obama s Justice Department. Hollywood was a big donor to Obama, and Obama reciprocated by naming at least five former Recording Industry Association of America attorneys to posts in the Justice Department, which has been waging a crackdown on internet piracy. The Justice Department is looking for even more money in next year s budget to hire more intellectual-property prosecutors.

Without SOPA or PIPA, the Justice Department lacks any mechanism to prevent Americans from visiting sites that are on a domain not controlled by a U.S. corporation. Knowing that, the world s leading BitTorrent site, The Pirate Bay, recently switched its main site from a .org domain to .se, the handle for Sweden.

The Pirate Bay s lead is unlikely to be followed by the millions of non-U.S. companies that rely on .com, which remains the net s beachfront real estate, even if it is subject to being confiscated by the U.S.

But it is possible that the U.S. government s big-footing over dot-com domains in the name of fighting copyright could add more weight to the arguments of those who want to put the U.N. in charge of the internet s naming system. While that s not inevitably a bad thing, it could lead to a world where any .com might be seizable by any country, including Russia, Libya and Iran.

Still, don t expect Uncle Sam to give up its iron grip on .com without a fight.

=~=~=~=